

06.7.2004  
PCT/JP2004/009907日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

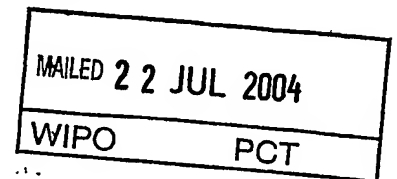
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 7月14日

出 願 番 号  
Application Number: 特願2003-273948

[ST. 10/C]: [JP2003-273948]

出 願 人  
Applicant(s): ソニー株式会社

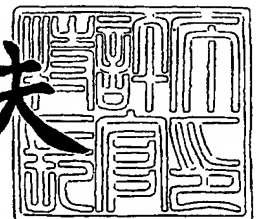


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 4月27日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願  
【整理番号】 0390350404  
【提出日】 平成15年 7月14日  
【あて先】 特許庁長官 今井 康夫 殿  
【国際特許分類】 H04L 9/06  
G06F 7/00

【発明者】  
【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内  
【氏名】 伊藤 雄二郎

【発明者】  
【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内  
【氏名】 下里 努

【発明者】  
【住所又は居所】 東京都品川区東五反田 2 丁目 2 0 番 4 号 ソニー・ヒューマンキ  
ャピタル株式会社内  
【氏名】 辻川 和伸

【特許出願人】  
【識別番号】 000002185  
【氏名又は名称】 ソニー株式会社

【代理人】  
【識別番号】 100082762  
【弁理士】  
【氏名又は名称】 杉浦 正知  
【電話番号】 03-3980-0339

【選任した代理人】  
【識別番号】 100120640  
【弁理士】  
【氏名又は名称】 森 幸一

【手数料の表示】  
【予納台帳番号】 043812  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 0201252

**【書類名】特許請求の範囲****【請求項 1】**

入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持手段と、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタと、

上記保持手段で保持された上記データと上記 1 または複数のカウンタによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

上記演算手段から出力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、

上記保持手段および上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする暗号装置。

**【請求項 2】**

請求項 1 に記載の暗号装置において、

上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記 1 または複数のカウント値とを暗号化するようにしたことを特徴とする暗号装置。

**【請求項 3】**

請求項 1 に記載の暗号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記 1 または複数のカウンタのうち少なくとも 1 の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする暗号装置。

**【請求項 4】**

請求項 1 に記載の暗号装置において、

上記入力データは映像データであって、上記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

**【請求項 5】**

請求項 4 に記載の暗号装置において、

上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

**【請求項 6】**

請求項 1 に記載の暗号装置において、

上記入力データは映像データであって、上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

**【請求項 7】**

請求項 6 に記載の暗号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする暗号装置。

**【請求項 8】**

請求項 6 に記載の暗号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

**【請求項 9】**

入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記デ

ータをリセット信号によりリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記 1 または複数のカウントのステップによる 1 または複数の上記カウント値とを暗号化する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記 1 または複数のカウントのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウントのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする暗号方法。

#### 【請求項 10】

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタと、上記保持手段で保持された上記データと上記 1 または複数のカウンタによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、上記演算手段から出力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、上記保持手段および上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された上記暗号化データを復号する復号装置において、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタと、

上記保持手段で保持された上記データと上記 1 または複数のカウンタによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

上記外部から入力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、

上記保持手段および上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする復号装置。

#### 【請求項 11】

請求項 10 に記載の復号装置において、

上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記 1 または複数のカウント値とを暗号化するようにしたことを特徴とする復号装置。

#### 【請求項 12】

請求項 10 に記載の復号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記 1 また

複数のカウンタのうち少なくとも 1 の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする復号装置。

【請求項 13】

請求項 10 に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

【請求項 14】

請求項 13 に記載の復号装置において、

上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

【請求項 15】

請求項 10 に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

【請求項 16】

請求項 15 に記載の復号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする復号装置。

【請求項 17】

請求項 15 に記載の復号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

【請求項 18】

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタのステップと、上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法において、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタのステップと、

上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに

所定の規則および／またはタイミングで発生する信号発生ステップとを有することを特徴とする復号方法。

【書類名】 明細書

【発明の名称】 暗号装置および方法、ならびに、復号装置および方法

【技術分野】

【0001】

この発明は、高いデータ秘守性を保ちデータの同期外れに対する復元性も高い暗号装置および方法、ならびに、復号装置および方法に関する。

【背景技術】

【0002】

従来から、デジタルデータの窃取や改竄などの不正利用を防ぐために、伝送されるデジタルデータに対して暗号化処理を施す暗号化技術が実用化されている。図5は、デジタルデータの暗号化を行う一例の構成を概略的に示す。暗号化処理を施す前の元データを平文（プレーンテキスト）と称し、平文に暗号化ブロック200で暗号化が施されて暗号文（暗号化データ）が生成される。暗号文は、暗号化ブロック200に対応する復号化ブロック201により暗号を復号化され、元の平文に戻される。

【0003】

暗号化ブロック200に用いられる暗号化方式としては、例えばAES (Advanced Encryption Standard)やDES (Data Encryption Standard)が代表的である。AESおよびDESは、何れも秘密鍵と称される公開されない鍵を用いて平文を暗号化および暗号文の復号化を行う。例えば暗号化ブロック200がAESにより暗号化を行う場合、暗号化ブロック200に入力された平文に対して、秘密鍵である鍵202を用いて暗号化を施す。暗号化された暗号文は、伝送経路を経由して復号化ブロック201に供給され、暗号化の際に用いられたのと同じ鍵202を用いて復号化され、元の平文に戻される。これらAESやDESは、暗号化と復号化において共通の鍵を用いる共通鍵方式である。

【0004】

暗号化ブロック200および復号化ブロック201の構成としては、図6に一例が示されるような、暗号化回路や復号化回路としてAESやDESによる暗号器50（または復号器）をそのまま用いる構成が考えられる。この図6の構成は、ECB (Electronic Code book mode)モードと称される。図6の構成において、暗号器50は、入力された平文Miを、鍵(K)を用いて例えばAESにより暗号化して暗号文Ciを得る。同一の構成において、暗号文Ciを暗号器50に入力し鍵(K)を用いて暗号化すると、暗号文Ciが復号化されて元の平文Miが得られる。

【0005】

この図6の構成では、同一の平文が連続的に入力されると、出力される暗号文も同一の値が続いてしまい、平文と暗号文とに基づく鍵(K)の解読が容易になってしまう。この問題を解決するために、様々な手法が考えられている。

【0006】

図7は、暗号器の出力を入力にフィードバックさせる構成であって、CBCモード(Cipher Block Chaining mode)と称する。図7Aに示される暗号化回路60においては、平文MiがEXOR（排他論理和）回路61を介して暗号器62に入力され、鍵(K)を用いて暗号化される。暗号器62の出力は、暗号文Ciとして出力されると共に、初期値IVとして遅延回路63により所定の、例えば1ワード分の遅延を与えられてEXOR回路61に供給され、平文Miとの排他論理和がとられる。このEXOR回路61の出力が暗号器62に入力される。

【0007】

図7Bは、対応する復号化回路65の構成を示す。復号化の際には、暗号文Ciを暗号器62に入力すると共に、初期値IV（イニシャライズベクタ）として遅延回路67で所定の、例えば1ワード分の遅延を与えてEXOR68に供給する。暗号文Ciは、暗号器62で鍵(K)を用いて暗号化され、EXOR68により、所定に遅延された初期値IVとの排他論理和をとられて元の平文Miに復号化され、出力される。

【0008】

この図 7 に示す構成によれば、初期値  $IV$  を変えることで、同一の鍵 ( $K$ ) を用いても、同一の平文  $M_i$  から異なる暗号文  $C_i$  が生成される。初期値  $IV$  として平文  $M_i$  を暗号化した暗号文  $C_i$  を用いているので、同一の平文  $M_i$  が連続的に入力されても暗号器 62 で暗号化された暗号文  $C_i$  は、同一とはならず、上述の ECB モードに比べて暗号文解析が難しくなる。

#### 【0009】

図 8 は、発生した暗号文  $C_i$  の一部を暗号器の入力としてフィードバックさせる構成であって、CFB モード (Cipher Feedback mode) と称する。図 8 A に示される暗号化回路 70 においては、 $j$  ビットデータとして入力された平文  $M_i$  が EXOR 回路 71 に供給され、暗号器 74 の出力のうち  $j$  ビットと排他論理和がとられ、暗号文  $C_i$  として出力される。この出力は、ビット数を  $j$  ビットから  $k$  ビットに変換する  $\varepsilon$  回路 72 を介して DR 回路 73 に供給される。DR 回路 73 は、シフトレジスタを有し、入力された  $k$  ビットのデータを入力順にシフトさせ、例えば 128 ビットのデータ  $X_i$  を発生させる。データ  $X_i$  は、暗号器 74 に供給され、鍵 ( $K$ ) を用いて暗号化され 128 ビットのデータ  $Y_i$  とされる。このデータ  $Y_i$  は、擬似的な乱数列であって、入力される平文  $M_i$  とで排他論理和をとることで、暗号文  $C_i$  が生成される。

#### 【0010】

図 8 B は、対応する復号化回路 75 の構成を示す。 $j$  ビットデータとして入力された暗号文  $C_i$  は、 $\varepsilon$  回路 76 で  $k$  ビットデータに変換され DR 回路 78 に供給されると共に、EXOR 回路 77 に供給される。DR 回路 78 は、シフトレジスタを有し、供給された  $k$  ビットのデータから例えば 128 ビットのデータ  $X_i$  を生成し、暗号器 79 に供給する。データ  $X_i$  は、暗号器 79 で鍵 ( $K$ ) を用いて暗号化され 128 ビットのデータ  $Y_i$  とされる。このデータ  $Y_i$  は、擬似的な乱数列であって、入力された暗号文  $C_i$  との排他論理和をとることで暗号文  $C_i$  が元の平文  $M_i$  に復号化される。

#### 【0011】

この CFB モードは、入力された平文  $M_i$  や暗号文  $C_i$  をシフトレジスタに入力し、それを暗号器に入力して疑似乱数列を発生させるので、連続的に平文  $M_i$  が入力されるストリームデータの暗号化に適している一方、暗号化回路 75 から出力された暗号化データに例えば伝送系などでエラーが生ずると、シフトレジスタ (DR 回路) が一巡するまでエラーから回復できないという欠点がある。

#### 【0012】

図 9 は、暗号器の出力だけをフィードバックして疑似乱数を発生させる構成であって、OFB モード (Output Feedback mode) と称する。図 9 A に示される暗号化回路 80 では、暗号器 83 自身の出力をシフトレジスタを有する DR 回路 82 を介して暗号器 83 に入力し、それを鍵 ( $K$ ) を用いて暗号化する。暗号器 83 から出力されたデータ  $Y_i$  は、疑似乱数列であって、このデータ  $Y_i$  のうち  $j$  ビットだけを EXOR 81 回路に供給し、 $j$  ビットデータとして入力される平文  $M_i$  との排他論理和をとることで、平文  $M_i$  が暗号文  $C_i$  とされ出力される。

#### 【0013】

図 9 B は、対応する復号化回路 85 の構成を示す。この OFB モードでは、復号化回路 85 は暗号化回路 80 と同一の構成とされる。すなわち、 $j$  ビットの暗号文  $C_i$  が EXOR 回路 86 に入力される。一方、暗号器 88 自身の出力がシフトレジスタを有する DR 回路 87 を介して暗号器 88 に入力され、鍵 ( $K$ ) を用いて暗号化される。暗号器 88 から出力されたデータ  $Y_i$  は、疑似乱数列であって、このデータ  $Y_i$  のうち  $j$  ビットだけを EXOR 86 に供給し、入力された暗号文  $C_i$  との排他論理和をとることで、暗号文  $C_i$  が平文  $M_i$  に復号化される。

#### 【0014】

この OFB モードは、暗号化回路 80 内および復号化回路 85 内でフィードバックが完結しているため、伝送系エラーなどの影響を受けないというメリットがある。

#### 【0015】



図10は、カウンタの出力を順次カウントアップしていき、それを暗号器の入力に与える構成であって、カウンタモードと称される。すなわち、カウンタモードでは、カウンタの出力が暗号化されて用いられる。図10Aに示される暗号化回路90では、128ビット出力のカウンタ92が順次カウントアップされたカウント値 $X_i$ が暗号器93に輸入され、鍵(K)を用いて暗号化される。暗号器93から出力されるデータ $Y_i$ は、疑似乱数列であって、このデータ $Y_i$ のうちjビットだけをEXOR回路91に供給し、jビットで入力された平文 $M_i$ との排他論理和をとることで、暗号文 $C_i$ が生成される。

#### 【0016】

図10Bは、対応する復号化回路95の構成を示す。このカウンタモードでは、復号化回路95は暗号化回路90と同一の構成とされる。すなわち、カウンタ97で順次カウントアップされたカウント値 $X_i$ が暗号器98に輸入され、A<sub>k</sub>ぎ(K)を用いて暗号化される。暗号器98から出力されるデータ $Y_i$ は、疑似乱数列であって、このデータ $Y_i$ のうちjビットだけをEXOR回路96に供給し、jビットで入力された暗号文 $C_i$ との排他論理和をとることで、暗号文 $C_i$ が平文 $M_i$ に復号化される。

#### 【0017】

上述のように、CFBモード、OFBモードおよびカウンタモードでは、暗号文 $C_i$ は、暗号化を行った同一の疑似乱数と暗号文 $C_i$ との排他論理和をとることで、復号化される。非特許文献1に、上述したような種々の暗号化方式が記載されている。

【非特許文献1】Douglas R. Stinson、櫻井幸一、「暗号理論の基礎」、共立出版株式会社、1996年

#### 【0018】

ところで、近年では、映画館などにおいて、例えば映像サーバに蓄積された映像データを再生し、スクリーンに投影して映画の上映を行うようにした、デジタルシネマシステムが提案されている。このシステムによれば、例えばネットワークを介して配信された映像データや、大容量光ディスクなどの記録媒体に記録された映像データが映像サーバに供給される。そして、映像サーバからプロジェクタに対して例えば同軸ケーブルを介してこの映像データが伝送され、プロジェクタによりスクリーンに映像データに基づく映像が投影される。

#### 【0019】

映像データは、例えばHD-SDI (High Definition-Serial Data Interface)による伝送フォーマットにより、シリアルデジタルデータとして映像サーバからプロジェクタに伝送される。この映像データは、ベースバンドのビデオデータとして伝送され、その伝送レートは、例えば略1.5 Gbps (Giga bits per second)とされる。

#### 【0020】

このとき、映像データの窃取を防ぐために、映像サーバから出力される映像データを暗号化し、暗号化された映像データを例えば同軸ケーブルに対して出力してプロジェクタに伝送する。ここで、HD-SDIのフォーマットにおいて伝送されるコードに制約が無ければ、上述した各暗号化方式を用い、HD-SDIの暗号化/復号化システムが実現できることになる。すなわち、映像サーバ側に暗号化回路を設け、出力される映像データに暗号化を施す。また、プロジェクタ側に映像サーバの暗号化回路に対応する復号化回路を持たせる。映像サーバで暗号化された映像データは、HD-SDIのフォーマットに乗せられて同軸ケーブルを介してプロジェクタに伝送され、プロジェクタの復号化回路で暗号を復号化され、ベースバンドのビデオデータに戻される。

#### 【0021】

しかしながら、実際には、上述のHD-SDIには、ワード同期用に禁止コードが定義されている。そこで、本願発明の出願人により、この禁止コードを発生させないで暗号化を行う方式が特願2002-135039として既に出願されている。また、当該出願の関連出願として、特願2002-135079、特願2002-135092、特願2002-173523および特願2002-349373が既に出願されている。

#### 【0022】

さらに、近年では、HD-SDIにおけるビデオデータの暗号化／復号化に関する標準化が進められており、暗号化方式として、図10を用いて説明したカウンタモードを用いることが提案されている。この提案によれば、暗号化単位の128ビットのデータを分割して用い、分割されたそれぞれのビットに対して下記の3種類のカウンタを適用するようにしている。

- (1) 暗号器のクロック毎にカウントアップするクロックカウンタ
- (2) 映像データのライン毎にカウントアップするラインカウンタ
- (3) 映像データのフレーム毎にカウントアップするフレームカウンタ

#### 【0023】

これら3種類のカウンタのうち(1)のクロックカウンタは、ラインが更新される毎にリセットされ、(2)のラインカウンタは、フレームが更新される毎にリセットされ、(3)のフレームカウンタは、映像データによる1つのプログラムの開始時に一度だけリセットされる。このように、カウント周期およびリセットタイミングが異なる複数のカウンタを組み合わせて用いることで、例えばデータの伝送系において同期外れ、データ欠落などが生じて、失われるすなわち復号できないデータは、最大で1ライン分のデータで済ませることができる。

#### 【0024】

また、(1)のクロックカウンタや(2)のラインカウンタによるリセットを行っても、(3)のフレームカウンタの値が更新されていくので、同一の疑似乱数列が繰り返されることが無いという利点もある。

#### 【0025】

これに対して、図8を用いて説明したCFBモードを用いる場合には、若し、プログラム開始後のある時点でリセットをかけ、その後リセットをかけないとしたら、上述した同期外れや、データの欠落などの事故が発生した場合、復帰が非常に困難である。つまり、このCFBモードにおいては、暗号化回路の出力をシフトレジスタにより順次シフトさせていったデータを暗号器で鍵(K)を用いて暗号化し、この暗号器の出力を用いて平文M<sub>i</sub>の暗号化を行っている。そのため、暗号化の際にある時点でエラーが発生すると、シフトレジスタによる影響が無くなるまで復号可能なデータが出力されない。換言すれば、CFBモードにおいては、出力される暗号文C<sub>i</sub>は、過去の全ての暗号文C<sub>i</sub>に依存しているため、短時間に復元することができない。

#### 【0026】

勿論、CFBモードでも、フレーム毎、ライン毎に暗号器の入力をリセットすることが可能である。しかしながら、CFBモードでフレーム毎、ライン毎にリセットを行った場合、例えば画面全体が黒一色といった均一な入力データが複数フレームにわたって入力された場合には、暗号器から出力される疑似乱数列は、フレーム毎に同一の並びとなってしまう。このようなケースが発生すると、例えば映像サーバとプロジェクタ間で伝送されるデータを窃取して暗号を解読する際の重大なヒントになってしまい、暗号のセキュリティ上、好ましくない。

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0027】

ここで、上述のデジタルシネマシステムにおける映像データの窃取方法について考える。図11は、この映像データ窃取を実現するための一例のシステムを概略的に示す。映像データは、映像サーバ250で再生されて暗号化され、暗号データとして同軸ケーブル251に送り出される。暗号化方式としては、伝送系のエラーに対する復元性を考慮し、上述したカウンタモードにおいて映像データのライン毎、フレーム毎、プログラムの先頭でそれぞれカウンタをリセットする方式を用いる。プロジェクタ254側では、本来であれば、プロジェクタ254に接続された同軸ケーブル251を介して送られてくるデータを受け取り、暗号を復号化してベースバンドの映像データとし、スクリーン255に映出する。

## 【0028】

映像データの窃取者は、データ窃取記録／交換装置252、ビデオカメラ256およびビデオデータ記録装置257を用意する。データ窃取記録／交換装置252は、映像サーバ250およびプロジェクタ254の間に挿入する。例えば、図11に示されるように、サーバ250とプロジェクタ254とを接続すべき同軸ケーブル251をデータ窃取記録／交換装置252に接続し、データ窃取記録／交換装置252の出力を同軸ケーブル253でプロジェクタ254に送る。ビデオカメラ256は、スクリーン255に投影された映像を撮影可能に配置される。ビデオカメラ256で撮影された映像は、ビデオデータ記録装置257に供給され、光ディスクや磁気テープなどの記録媒体に記録される。

## 【0029】

このような構成において、窃取者は、映像サーバ250から出力される、映像データが暗号化された暗号化データと、映像データに付随するメタデータとをデータ窃取記録／交換装置252で記録する。データ窃取記録／交換装置252は、映像サーバ250から供給された暗号化データの代わりに、予め用意した所定データを、映像サーバ250から暗号化データに付随されて供給されたメタデータと共に出力する。このとき、メタデータには手を加えない。なお、データ窃取記録／交換装置252で予め用意される所定データは、例えば黒一色の画面を表示するための固定値である。

## 【0030】

データ窃取記録／交換装置252から出力された所定データとメタデータは、プロジェクタ254に供給される。プロジェクタ254では、供給された所定データを復号化する。すなわち、所定データが黒一色を表示する固定データである場合、所定データと復号化回路における疑似乱数とが排他論理和演算される。この所定データと疑似乱数とが排他論理和演算されてなる映像データがスクリーン255に投影される。

## 【0031】

スクリーン255に投影される映像は、このように、例えば固定値である所定データに暗号化回路による疑似乱数を作用させたデータに基づくので、絵としては映像サーバ250から出力された元の映像データとは全く異なり、ノイズとしか見えないような映像となる。窃取者は、このスクリーン255に投影された上述の所定データによる映像をビデオカメラ256で撮影し、ビデオデータ記録装置257で記録する。このデータ窃取記録／交換装置252で記録された暗号化データと、ビデオデータ記録装置257で記録された映像データとに基づき、暗号データ化の元の映像データを復元することができる。

## 【0032】

すなわち、プロジェクタ254の映写性能と、ビデオカメラ256の撮像性能とが理想的なものであれば、これら暗号化データと映像データの排他論理和をとることで、暗号化データの元の映像データを復元できることになるという問題点があった。

## 【0033】

現実的には、理想的な性能を備えたプロジェクタ254やビデオカメラ256は存在しないので、上述の方法でも、正確に元の映像データを復元することはできない。しかしながら、不完全なデータを用いても、上述の演算を行うことで、高い確率で元の映像データの再現を行うことが可能である。

## 【0034】

例えば、映像データの性質として、ある画素とその画素に近接した画素とでは、高い相関性があることが知られている。この近接画像の相関性を利用して、上述のような状況下において、正確に再現できなかった画素の値を求めることができる。その結果、その画素（映像データ）を暗号化した際の疑似乱数を絞り込んでいくことができてしまう。これにより、窃取者により、映像データの暗号化の際の鍵（K）を解読する大きな手がかりを得られてしまうという問題点があった。

## 【0035】

一方、映像サーバ250から出力される映像データに対して暗号化を行う暗号化方式としてCFBモードを用いれば、この方式では暗号化された暗号化データをフィードバック

して入力データの暗号化を行っているため、同一のデータを入力し続けても出力される疑似乱数列が変化する。そのため、上述のような窃取方法では鍵 (K) の手がかりを得ることが困難である。しかしながら、上述したように、CFBモードは、伝送系のエラーに対する復元性が弱いという問題点があった。これは、実際に映画館での上映などに用いる際に、深刻な問題となりうる。

#### 【0036】

したがって、この発明の目的は、より秘守性に優れ、尚かつ、伝送系のエラーに対する復元性も高い暗号化を行うことができる暗号装置および方法、ならびに、復号装置および方法を提供することにある。

#### 【課題を解決するための手段】

#### 【0037】

この発明は、上述した課題を解決するために、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタと、保持手段で保持されたデータと1または複数のカウンタによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および1または複数のカウンタのそれぞれに所定の規則および/またはタイミングで発生する信号発生手段とを有することを特徴とする暗号装置である。

#### 【0038】

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および/またはタイミングで発生する信号発生ステップとを有することを特徴とする暗号方法である。

#### 【0039】

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタと、保持手段で保持されたデータと1または複数のカウンタによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および1または複数のカウンタのそれぞれに所定の規則および/またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された暗号化データを復号する復号装置において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1

または複数のカウンタと、保持手段で保持されたデータと1または複数のカウンタによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、外部から入力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする復号装置である。

#### 【0040】

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データを暗号化データとして出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号方法で暗号化された暗号化データを復号する復号方法において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする復号方法である。

#### 【0041】

上述したように、この発明では、最終的な暗号化データの一部または全部がトリガ信号により保持されリセット信号によりリセットされる保持された暗号化データとトリガ信号によりカウント値をカウントアップまたはカウントダウンしリセット信号によりカウント値が所定の値にリセットされる1または複数のカウント値とを暗号化した出力と、外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化して最終的な暗号化データとして出力するようにされ、最終的な暗号化データが暗号化されるデータにフィードバックされると共に、暗号化データを得るための演算に用いる暗号化の出力がリセット信号によりリセットされるため、同一データの連続入力を利用したデータ窃取が行えないと共に、暗号化データの伝送系によるデータエラーなどに対する復元力を有する。

#### 【発明の効果】

#### 【0042】

この発明によれば、暗号化回路にCFBモードを取り入れ、ビデオデータの暗号化の際に、出力された暗号化データを暗号器の入力にフィードバックしているため、従来技術で図11を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができないという効果が

ある。これは、CFBモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と、暗号化回路において暗号器で発生される疑似乱数列とが全く異なるからである。

【0043】

また、この発明によれば、暗号化データを暗号器の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドし、ホールドされた暗号化データをライン毎にリセットしているため、前ラインでの暗号化データによるフィードバックの影響が全くなり、前ラインで同期外れや画素欠落などの事故が生じた場合でも、ラインが更新された際に完全に復帰できるという効果がある。

【発明を実施するための最良の形態】

【0044】

以下、この発明の実施の一形態を、図面を参照しながら説明する。図1は、この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示す。この映像投影システムは、デジタルデータとして提供された映像データを映画館などで上映する際に用いて好適なものである。ビデオデコーダ10は、例えば図示されない映像サーバからネットワークなどを介して供給された、圧縮符号化された映像データをデコードし、ベースバンドのビデオデータとする。このビデオデータは、例えばHD-SDIのフォーマットに乗せられ、伝送レートが略1.5 Gbpsのシリアルデジタルデータとして出力される。

【0045】

なお、ビデオデコーダ10は、例えば大容量の光ディスクといった記録媒体に圧縮符号化されて記録された映像データをビデオデコーダ10で再生し、デコードして出力するようにしてもよい。

【0046】

ビデオデコーダ10から出力されたデータは、同軸ケーブル11を介してHD-SDI暗号化装置12に供給される。HD-SDI暗号化装置12は、供給されたデータから映像データを抽出して暗号化を施し、暗号化ビデオデータとし、この暗号化ビデオデータを再びHD-SDIのフォーマットに乗せて出力する。暗号化の際の鍵(K)は、例えば、RS232Cなどのインターフェイスを介して接続されたコンピュータ装置(PC)から供給される。HD-SDI暗号化装置12から出力されたデータは、同軸ケーブル13を介してプロジェクタ16側に伝送され、HD-SDI復号化装置14に供給される。

【0047】

HD-SDI復号化装置14は、HD-SDIフォーマットのデジタルデータから暗号化ビデオデータを抽出して暗号を復号化し、元のベースバンドのビデオデータに戻す。復号化の際の鍵(K)は、HD-SDI暗号化装置12において暗号化の際に用いられた鍵(K)と共通の鍵が用いられ、例えば、RS-232Cなどのインターフェイスを介して接続されたコンピュータ装置から供給される。

【0048】

HD-SDI復号化装置14で復元されたベースバンドのビデオデータは、同軸ケーブル15を介してプロジェクタ16に供給され、プロジェクタ16により図示されないスクリーンに投影される。

【0049】

なお、上述では、ビデオデコーダ10とHD-SDI暗号化装置12とが別個の装置であるように説明したが、実際には、HD-SDI暗号化装置12は、ビデオデコーダ10に組み込まれて用いられる。この場合には、ビデオデコーダ10とHD-SDI暗号化装置12とを接続する同軸ケーブル11を省略することができ、また、ビデオデコーダ10から出力されるビデオデータをHD-SDIのフォーマットに乗せず、例えばパラレルのデジタルデータとして扱うことができる。HD-SDI復号装置14も同様に、プロジェクタ16に組み込まれて用いられる。この場合にも同様に、同時期ケーブル15を省略することができると共に、HD-SDI復号装置14からパラレルデジタルデータ



タとしてビデオデータを出力することができる。

【0050】

図2は、HD-SDI暗号化装置12の一例の構成を示す。HD-SDI暗号化装置12は、概略的には、HD-SDIシリアル/パラレル変換回路ブロック20、暗号回路ブロック30およびHD-SDIパラレル/シリアル変換回路ブロック40から構成される。

【0051】

HD-SDIフォーマットに乗せられ、同軸ケーブル11を介して伝送されたデジタルデータは、HD-SDIシリアル/パラレル変換回路ブロック20に供給されてパラレルのデジタルデータに変換され、ビデオデータ、オーディオデータおよびメタデータが取り出される。オーディオデータおよびメタデータは、HD-SDIパラレル/シリアル変換回路ブロック40に供給され、ビデオデータは、暗号化回路ブロック30で暗号化されてHD-SDIパラレル/シリアル変換回路ブロック40に供給される。HD-SDIパラレル/シリアル変換回路ブロック40では、オーディオデータおよびメタデータと、暗号化された暗号化ビデオデータとを重畳し、HD-SDIフォーマットに準じたシリアルデジタルデータに変換して出力する。

【0052】

HD-SDIシリアル/パラレル変換回路ブロック20において、入力されたHD-SDIフォーマットのシリアルデジタルデータは、ケーブルイコライザ(EQ)/クロック復元回路21で、伝送時に同軸ケーブル11により劣化した周波数特性が補正されると共に、クロックが抽出される。デジタルデータは、受信時に信号が反転しても受信可能なように、NRZI符号化されて信号の方向性が除去されている。ケーブルイコライザ/クロック復元回路21から出力されたデジタルデータは、NRZI回路22に供給され、送信時に施されたNRZI符号が復号化される。NRZI回路22の出力は、デスクランブラ23でデータの送信時にDC成分を除去するために施されたスクランブル処理が解除され、シンク検出回路24でワード同期が検出され、検出されたワード同期に基づきシリアル/パラレル変換回路25でパラレルのデジタルデータに変換される。

【0053】

シリアル/パラレル変換回路25の出力は、デマルチプレクサ26に供給され、多重化されているビデオデータ、オーディオデータおよびメタデータなどが分離される。デマルチプレクサ26で分離されたオーディオデータおよびメタデータは、HD-SDIパラレル/シリアル変換回路ブロック40のマルチプレクサ/フォーマッタ41に供給される。

【0054】

一方、デマルチプレクサ26で分離されたビデオデータは、暗号回路ブロック30に供給され、暗号化回路31で暗号化される。暗号回路ブロック30は、CPU(Central Processing Unit)32を有し、例えばRS-232Cといった所定のインターフェイスを介して外部のコンピュータ装置と通信を行うことができる。暗号化回路31において暗号化の際に用いられる鍵(K)は、外部のコンピュータ装置から所定のインターフェイスを介して供給され、CPU32を介して暗号化回路31に与えられる。暗号化回路31で暗号化された暗号化ビデオデータは、HD-SDIパラレル/シリアル変換回路ブロック40のマルチプレクサ/フォーマッタ41に供給される。

【0055】

HD-SDIパラレル/シリアル変換回路ブロック40において、マルチプレクサ/フォーマッタ41は、供給されたオーディオデータ、メタデータおよび暗号化ビデオデータを多重化し、HD-SDIフォーマットにマッピングする。マルチプレクサ/フォーマッタ41の出力は、パラレル/シリアル変換回路42でシリアルデジタルデータに変換され、スクランブラ43でスクランブル処理されDC成分を除去され、NRZI回路44で上述したNRZI符号化される。NRZI回路44の出力は、ケーブルドライバ45で伝送レベルまで増幅され、同軸ケーブル13に対して送り出される。

【0056】

なお、HD-SDI復号化装置14は、このHD-SDI暗号化装置12におけるHD-SDIシリアル/パラレル変換回路ブロック20と同様の回路(HD-SDIシリアル/パラレル変換回路ブロック20'とする)と、暗号回路ブロック30に対応する復号回路ブロックとを有する。同軸ケーブル13を介して供給されたHD-SDIフォーマットのデジタルデータは、HD-SDIシリアル/パラレル変換回路ブロック20'において上述のHD-SDIシリアル/パラレル変換回路ブロック20と同様の処理がなされ、暗号化ビデオデータ、オーディオデータおよびメタデータが取り出される。暗号化ビデオデータは、復号回路ブロックに供給され外部のコンピュータ装置から供給された鍵(K)を用いて復号化され、ベースバンドのビデオデータが復元される。復元されたデータのうち、ビデオデータおよびメタデータは、プロジェクト16に供給される。また、オーディオデータは、図示されないオーディオシステムに供給される。

#### 【0057】

図3は、この発明の実施の一形態による暗号化回路31の一例の構成を示す。この発明の実施の一形態による暗号化回路31は、カウンタモードによるデータエラーからの復元性と、CFBモードによる、データ窃取に対する堅牢性とを兼ね備えた構成を実現している。

#### 【0058】

暗号器105は、128ビットの長さの鍵(K)を用いてAESによる暗号化を施すAES暗号器である。なお、暗号器105において利用可能な暗号化方式は、AESに限られない。DESなどのデータをブロック化して暗号化する方式であれば、他の暗号化方式を用いることもできる。また、鍵(K)のデータ長も128ビットに限定されない。

#### 【0059】

CPU+タイミングコントローラ110は、図2に示したCPU32と、図示されないタイミングコントローラからなる。タイミングコントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

#### 【0060】

暗号化回路31に対して、1画素分のデータが輝度Yおよび色差Cそれぞれ10ビットずつを割り当てたデータ幅が20ビットからなるビデオデータが、クロック毎に1画素ずつ入力される。このビデオデータは、EXOR回路100に供給され、後述するP/Pシフトレジスタ106の出力との排他論理和をとられ、暗号化ビデオデータとされて出力される。

#### 【0061】

EXOR回路100から出力された暗号化ビデオデータは、外部すなわちHD-SDIパラレル/シリアル変換回路ブロック40に対して出力される。それと共に、暗号化ビデオデータは、フリップフロップ(FF)回路101に供給され、ホールドされる。FF回路101は、AES暗号器105と同一のクロック107によりホールド値が更新される。また、FF回路101は、ビデオデータのラインが更新される毎に所定の回数リセットするように、CPU+タイミングコントローラ110からリセット信号119が供給される。リセット信号119の回数は、例えば、AES暗号器105へのリセット値がAES暗号器105の出力に反映される、AESレーテンシ分に対応した回数とされる。

#### 【0062】

なお、この実施の一形態では、FF回路101に対して、データ幅が20ビットの暗号化ビデオデータのうち一部、例えば16ビットだけが入力される。用いられる16ビットは、元の暗号化ビデオデータの20ビットのデータ幅のうちLSB側、MSB側のうち何れでもよいし、20ビットの中から所定の16ビットを用いてもよい。なお、これはこの例に限らず、FF回路101に対して暗号化ビデオデータの20ビット全てを入力することもできるし、16ビットより少ないビット数で入力するようにしてもよい。

#### 【0063】

ラインカウンタ102は、CPU+タイミングコントローラ110からビデオデータの



ライン毎に供給されるトリガ信号 118 によりカウント値を更新するカウンタである。例えば、ラインカウンタ 102 は、ビデオデータのライン毎に、カウント値を 1 だけカウントアップする。また、ラインカウンタ 102 は、フレームが更新される毎に 1 回リセットされるように、CPU+タイミングコントローラ 110 からリセット信号 117 が供給される。ラインカウンタ値は、例えば 16 ビットのデータである。

**【0064】**

なお、ラインカウンタ 102 は、この例に限られず、複数ライン毎にカウント値を更新するようにしてもよい。また、カウント値の更新も、1 ずつカウントするのに限られず、2 以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。さらに、リセット信号 117 によるリセットの際にカウント値が 0 になるようにリセットしてもよいし、0 以外の所定値になるようにリセットすることもできる。さらにまた、ラインカウンタ値のデータ長は 16 ビットに限られない。

**【0065】**

フレームカウンタ 103 は、CPU+タイミングコントローラ 110 からビデオデータのフレーム毎に供給されるトリガ信号 116 によりカウント値を更新するカウンタである。例えば、フレームカウンタ 103 は、ビデオデータのフレーム毎に、カウント値を 1 だけカウントアップする。フレームカウンタ 103 は、例えばビデオデータのプログラムの開始時に 1 回リセットするように、CPU+タイミングコントローラ 110 からリセット信号 114 が供給される。フレームカウンタ値は、例えば 24 ビットのデータである。

**【0066】**

なお、フレームカウンタ 103 は、この例に限られず、カウント値の更新を、1 ずつカウントするのに限られず、2 以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。また、リセット信号 117 によるリセットの際にカウント値が 0 になるようにリセットしてもよいし、0 以外の所定値になるようにリセットすることもできる。さらに、リセット信号 114 も、プログラムの先頭でリセットするのに限らず、例えば所定数のフレーム数毎にリセットするようなものでもよい。さらにまた、ラインカウンタ値のデータ長は 16 ビットに限られない。

**【0067】**

FF 回路 104 は、CPU+タイミングコントローラ 110 から与えられるデータ 112 をホールドする。このデータ 112 は、上述したフレームやラインのデータとは異なるデータであって、例えばバージョン情報といった固定値を用いてもよいし、所定の規則、例えばトリガ信号 113 に基づく所定のタイミングで更新される値であってもよい。FF 回路 104 の出力は、例えば 72 ビットのデータである。FF 回路 104 の出力は、リセット信号 111 により所定のタイミングでリセットすることができる。なお、FF 回路 104 の出力のデータ長は、72 ビットに限定されない。

**【0068】**

上述の FF 回路 104、フレームカウンタ 103、ラインカウンタ 102 および FF 回路 101 にそれぞれホールドされたデータは、AES 暗号器 105 のクロックタイミングで並列的に AES 暗号器 105 に読み出される。すなわち、この図 3 の例では、FF 回路 104 にホールドされた 72 ビットのデータと、フレームカウンタ 103 にホールドされた 24 ビットのデータと、ラインカウンタ 102 にホールドされた 16 ビットのデータと、FF 回路 101 にホールドされた 16 ビットのデータとからなる 128 ビットのデータが、AES 暗号器 105 のクロックタイミングで、AES 暗号器 105 に入力される。

**【0069】**

一方、CPU+タイミングコントローラ 110 から AES 暗号器 105 に対して、鍵長が 128 ビットの鍵 (K) が与えられる。AES 暗号器 105 は、上述の FF 回路 104、フレームカウンタ 103、ラインカウンタ 102 および FF 回路 101 から入力された 128 ビットのデータに対して、鍵 (K) を用いて暗号化を施す。暗号化されて得られた 128 ビットの暗号化データは、そのうちの所定の 120 ビットだけが P/P シフトレジスタ 106 に供給される。

## 【0070】

P/Pシフトレジスタ106は、供給された120ビットの暗号化データを、入力されるビデオデータのデータ幅に合わせて20ビットずつに分割する。したがって、AES暗号器105を動作させるためのクロックは、画像データに同期したクロックの1/6の周波数となっている。P/Pシフトレジスタ106から出力された20ビットのデータがEXOR回路100に供給される。EXOR回路100では、上述したように、入力されたビデオデータとP/Pシフトレジスタ106からの出力との排他論理和をとることで、入力されたビデオデータを暗号化して出力する。

## 【0071】

このように、この発明による暗号化回路31では、暗号化された暗号化データをAES暗号器105の入力にフィードバックしているため、従来技術で図11を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができない。これは、CFBモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と、暗号化回路31においてAES暗号器105で発生される疑似乱数列とが全く異なるからである。

## 【0072】

また、暗号化データをAES暗号器105の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドするFF回路104に対してライン毎のリセットを行っているため、前ラインでの暗号化データによるフィードバックの影響が全くなくなる。したがって、前ラインで同期外れや画素欠落などの事故が生じた場合、CFBモードでは当該ライン上にある暗号データの復号は不可能であるが、本発明の方式によれば、ラインが更新された際に完全に復帰できることを意味する。

## 【0073】

なお、上述では、AES暗号器105に入力されるデータをFF回路104、フレームカウンタ103、ラインカウンタ102およびFF回路101の出力としたが、これはこの例に限定されない。例えば、FF回路104による固定値出力を省略することができる。また、フレームカウンタ103およびラインカウンタ102に対して更新およびリセット周期が異なるカウンタをさらに追加してもよいし、フレームカウンタ103を省略することも可能である。さらに、上述では、FF回路104、フレームカウンタ103、ラインカウンタ102およびFF回路101の出力データのビット配分を、FF回路104が72ビット、フレームカウンタ103が24ビット、ラインカウンタ102およびFF回路101がそれぞれ16ビットとしたが、これはこの例に限定されず、他のビット配分でもよい。さらにまた、入力されるビデオデータのビット幅も、20ビットに限定されず、ビデオ信号の形式も輝度Y、色差Cによるものに限定されない。

## 【0074】

ここで、特許請求の範囲との一例の対応関係を示すと、請求項1において、保持手段は、例えばFF回路101に対応する。1または複数のカウンタは、例えばフレームカウンタ103およびラインカウンタ102に対応する。暗号化手段は、例えばAES暗号器105に対応する。演算手段は、例えばEXOR回路100に対応する。演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路は、例えばEXOR回路100の出力がFF回路101に供給される経路に対応する。信号発生手段は、例えばCPU+タイミングコントローラ110に対応する。なお、これらの対応関係は一例であって、これに限定されるものではない。

## 【0075】

図4は、図3に示す暗号化回路31に対応する復号化回路50の一例の構成を示す。この復号化回路50は、HD-SDI復号装置14に組み込まれて用いられ、HD-SDI暗号化装置12から同軸ケーブル13を介して伝送された暗号化ビデオデータを復号化する。復号化回路50は、暗号化回路31におけるFF回路101に対して入力される暗号化ビデオデータの入力経路が異なる以外、同一の構成で実現できる。また、復号化回路5

0において、各種のタイミングやデータのビット幅などは、上述の暗号化回路31と対応させられる。

**【0076】**

復号化回路50において、AES暗号器125は、上述した暗号化回路31で用いられるAES暗号器105と同一の回路であって、入力されたデータに対して、暗号化回路31と共通の鍵である128ビットの長さの鍵(K)を用いてAESによる暗号化を施す。また、CPU+タイミングコントローラ130は、CPUとタイミングコントローラからなる。タイミングコントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

**【0077】**

復号化回路50に対して、1画素分に対応する暗号化ビデオデータがデータ幅20ビットで以てクロック毎に入力される。この暗号化ビデオデータは、EXOR回路120に供給され、後述するP/Pシフトレジスタ126の出力との排他論理和をとられ、暗号化ビデオデータが復号化され元のデータが復元された復元ビデオデータとされて出力される。

**【0078】**

暗号化ビデオデータは、EXOR回路120に供給されると共に、20ビットのうち上述のFF回路101で用いられたのに対応する16ビットがFF回路121に供給され、ホールドされる。勿論、上述のFF回路101において入力ビデオデータの20ビットの全てが用いられた場合、FF回路121には、暗号化ビデオデータの20ビット全てが入力される。FF回路121は、AES暗号器125と同一のクロック127によりホールド値が更新される。また、FF回路121は、ビデオデータのラインが更新される毎に所定の回数リセットするように、CPU+タイミングコントローラ130からリセット信号139が供給される。リセット信号139のタイミングは、例えば、AES暗号器125へのリセット値がAES暗号器125の出力に反映される、AESレーテンシ分とされる。

**【0079】**

ラインカウンタ122は、上述のラインカウンタ102に対応して更新されるカウンタであり、CPU+タイミングコントローラ130から暗号化ビデオデータのライン毎に供給されるトリガ信号138により、例えば暗号化ビデオデータのライン毎にカウント値を1だけカウントアップしてカウント値を更新する。また、ラインカウンタ122は、フレームが更新される毎に1回リセットされるように、CPU+タイミングコントローラ130からリセット信号137が供給される。ラインカウント値は、例えば16ビットのデータである。

**【0080】**

フレームカウンタ123は、上述のフレームカウンタ103に対応して更新されるカウンタであり、CPU+タイミングコントローラ130から暗号化ビデオデータのフレーム毎に供給されるトリガ信号136により、例えば暗号化ビデオデータのフレーム毎にカウント値を1だけカウントアップしてカウント値を更新するカウンタである。フレームカウンタ123は、例えば暗号化ビデオデータのプログラムの開始時に1回リセットするように、CPU+タイミングコントローラ130からリセット信号134が供給される。フレームカウント値は、例えば24ビットのデータである。

**【0081】**

FF回路124は、CPU+タイミングコントローラ130から与えられるデータ132をホールドする。このデータ132は、上述のデータ112に対応する値が用いられる。FF回路124の出力は、例えば72ビットのデータである。FF回路124の出力は、上述のリセット信号111に対応するタイミングのリセット信号131によりリセットすることができる。

**【0082】**

上述のFF回路124、フレームカウンタ123、ラインカウンタ122およびFF回路121にそれぞれホールドされたデータは、AES暗号器125のクロックタイミング

で並列的にAES暗号器125に読み出される。すなわち、この図4の例では、FF回路124にホールドされた72ビットのデータと、フレームカウンタ123にホールドされた24ビットのデータと、ラインカウンタ122にホールドされた16ビットのデータと、FF回路121にホールドされた16ビットのデータとからなる128ビットのデータが、AES暗号器125のクロックタイミングで、AES暗号器125に入力される。

**【0083】**

一方、CPU+タイミングコントローラ130からAES暗号器125に対して、鍵長が128ビットの鍵(K)が与えられる。この鍵(K)は、上述した暗号化回路31で用いられる鍵(K)と共通する鍵である。AES暗号器125は、上述のFF回路124、フレームカウンタ123、ラインカウンタ122およびFF回路121から入力された128ビットのデータに対して、鍵(K)を用いて暗号化を施す。暗号化されて得られた128ビットの暗号化データは、そのうちの所定の120ビットだけがP/Pシフトレジスタ126に供給される。

**【0084】**

P/Pシフトレジスタ126は、供給された120ビットの暗号化データを、入力される暗号化ビデオデータのデータ幅に合わせて20ビットずつに分割する。したがって、AES暗号器125を動作させるためのクロックは、画像データに同期したクロックの1/6の周波数となっている。P/Pシフトレジスタ126から出力された20ビットのデータがEXOR回路120に供給される。EXOR回路120では、上述したように、入力された暗号化ビデオデータとP/Pシフトレジスタ126からの出力との排他論理和をとることで、入力された暗号化ビデオデータを復号化して出力する。

**【0085】**

上述したように、この復号化回路50は、上述の暗号化回路31に対応するものである。したがって、AES暗号器125にデータを入力するFF回路124、フレームカウンタ123、ラインカウンタ122およびFF回路121の構成や動作は、上述の暗号化回路31におけるFF回路104、フレームカウンタ103、ラインカウンタ102およびFF回路101に対応する。

**【0086】**

ここで、特許請求の範囲との一例の対応関係を示すと、請求項10において、保持手段は、例えばFF回路121に対応する。1または複数のカウンタは、例えばフレームカウンタ123およびラインカウンタ122に対応する。暗号化手段は、例えばAES暗号器125に対応する。演算手段は、例えばEXOR回路120に対応する。外部から入力された暗号化データの一部または全部を保持手段に入力する経路は、例えば暗号化ビデオデータがEXOR回路120に入力されると共にFF回路121に供給される経路に対応する。信号発生手段は、例えばCPU+タイミングコントローラ130に対応する。なお、これらの対応関係は一例であって、これに限定されるものではない。

**【0087】**

なお、ここでは、入力されたビデオデータに対してP/Pシフトレジスタ106の出力を作用させ、暗号化ビデオデータを得るためにEXOR回路100を用いているが、これはこの例に限定されない。

**【0088】**

また、上述では、ビデオデータ、暗号化ビデオデータの伝送をHD-SDIの規格に基づき行うように説明したが、これはこの例に限定されるものではなく、この発明は、他の伝送方式に対しても適用可能である。

**【図面の簡単な説明】****【0089】**

【図1】この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示すブロック図である。

【図2】HD-SDI暗号化装置の一例の構成を示すブロック図である。

【図3】この発明の実施の一形態による暗号化回路の一例の構成を示すブロック図で

ある。

【図4】この発明の実施の一形態による暗号化回路に対応する復号化回路の一例の構成を示すブロック図である。

【図5】デジタルデータの暗号化を行う一例の構成を概略的に示すブロック図である。

【図6】ECBモードによる暗号化回路の一例の構成を示すブロック図である。

【図7】CBCモードによる暗号化回路の一例の構成を示すブロック図である。

【図8】CFBモードによる暗号化回路の一例の構成を示すブロック図である。

【図9】OFBモードによる暗号化回路の一例の構成を示すブロック図である。

【図10】カウンタモードによる暗号化回路の一例の構成を示すブロック図である。

【図11】映像データ窃取を実現するための一例のシステムを概略的に示すブロック図である。

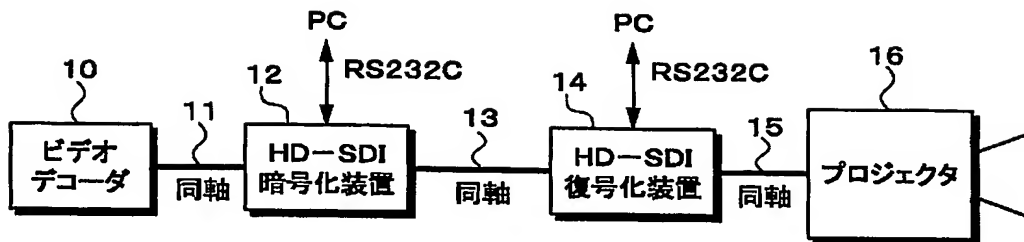
【符号の説明】

【0090】

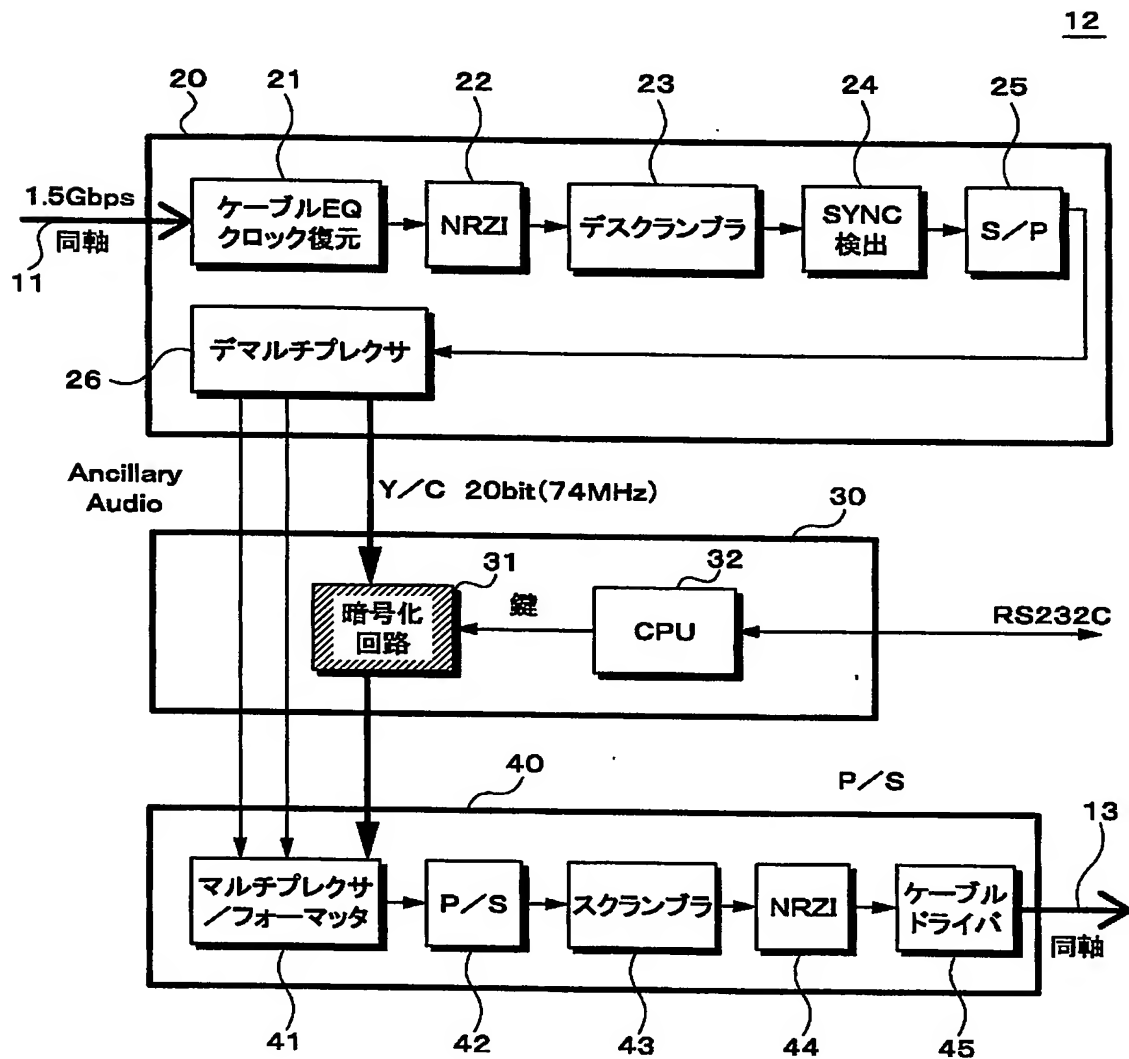
- 10 ビデオデコーダ
- 12 HD-SDI暗号化装置
- 13 同軸ケーブル
- 14 HD-SDI復号装置
- 16 プロジェクタ
- 20 HD-SDIシリアル／パラレル変換回路ブロック
- 26 デマルチプレクサ
- 30 暗号回路ブロック
- 31 暗号化回路
- 32 CPU
- 40 HD-SDIパラレル／シリアル変換回路ブロック
- 41 マルチプレクサ／フォーマッタ
- 50 復号化回路
- 100 EXOR回路
- 101 FF回路
- 102 ラインカウンタ
- 103 フレームカウンタ
- 104 FF回路
- 105 AES暗号器
- 106 P／Pシフトレジスタ
- 110 CPU＋タイミングコントローラ

【書類名】 図面

【図 1】

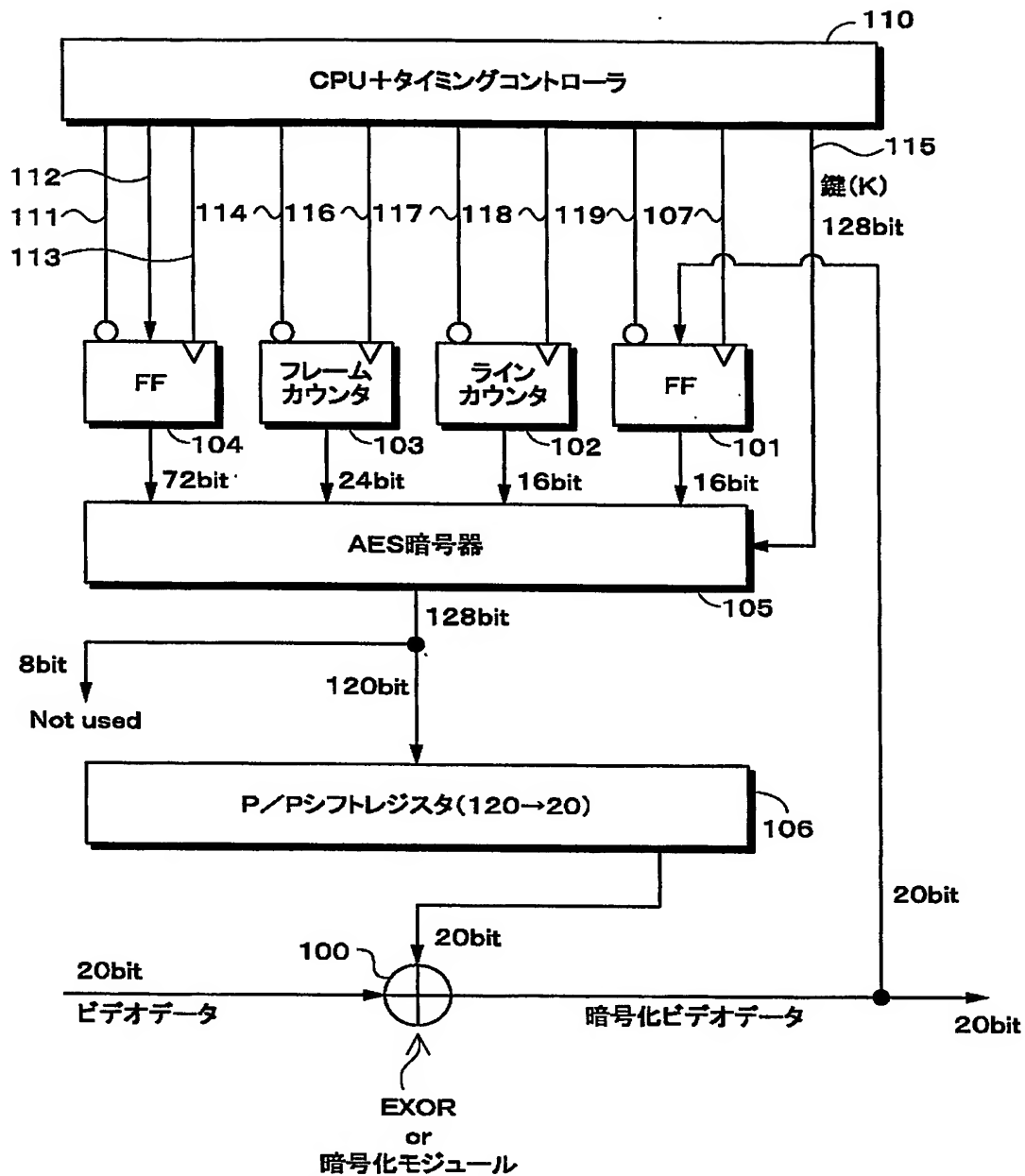


【図 2】

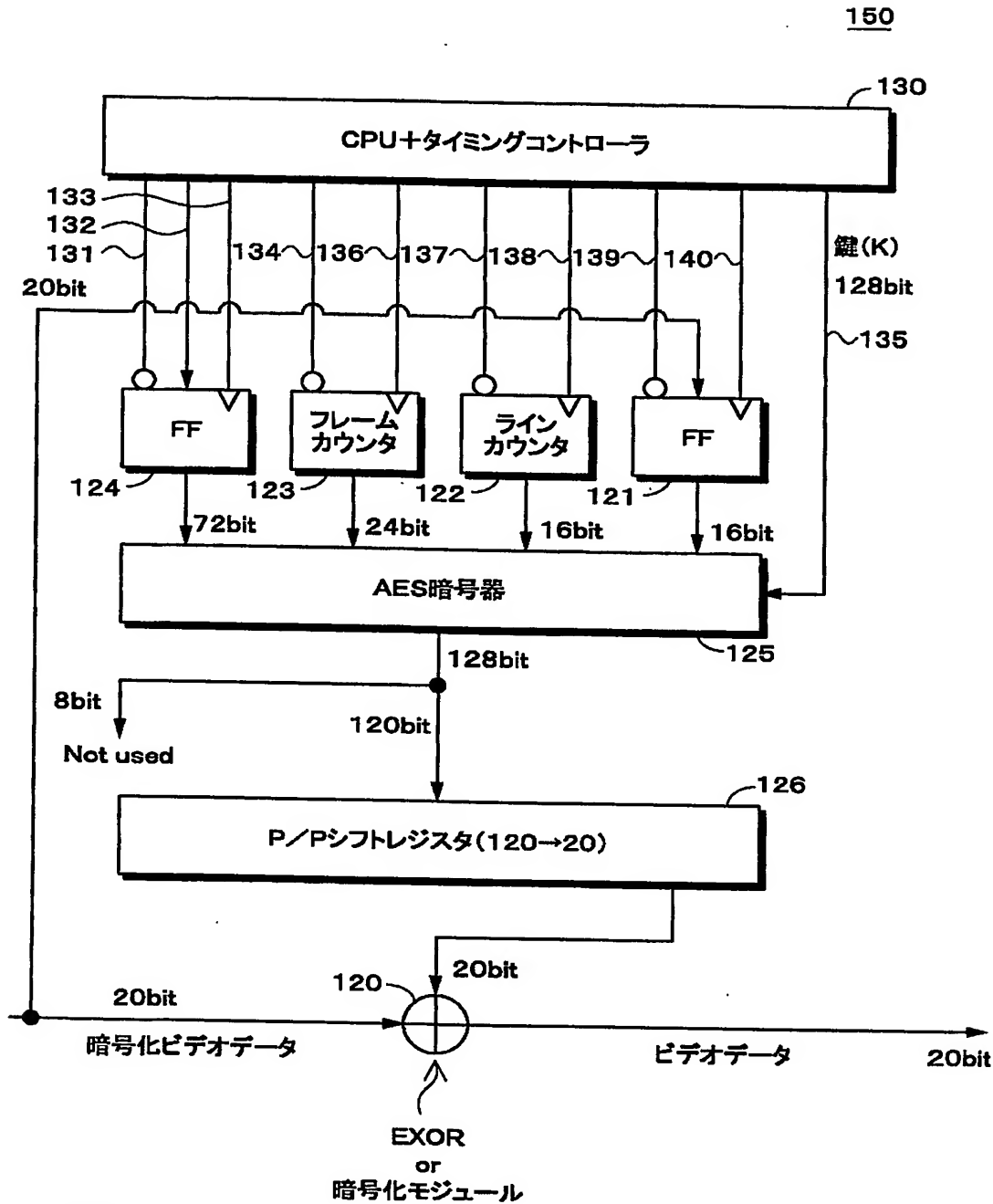


【図 3】

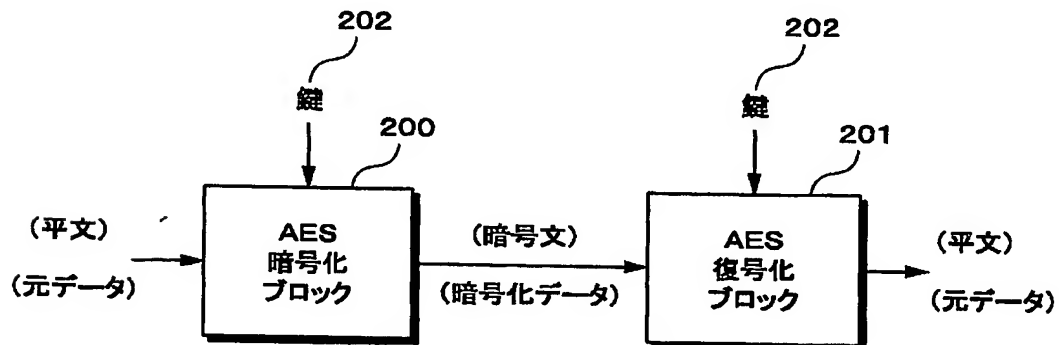
31



【図 4】

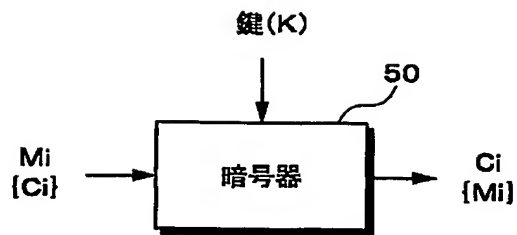


【図 5】

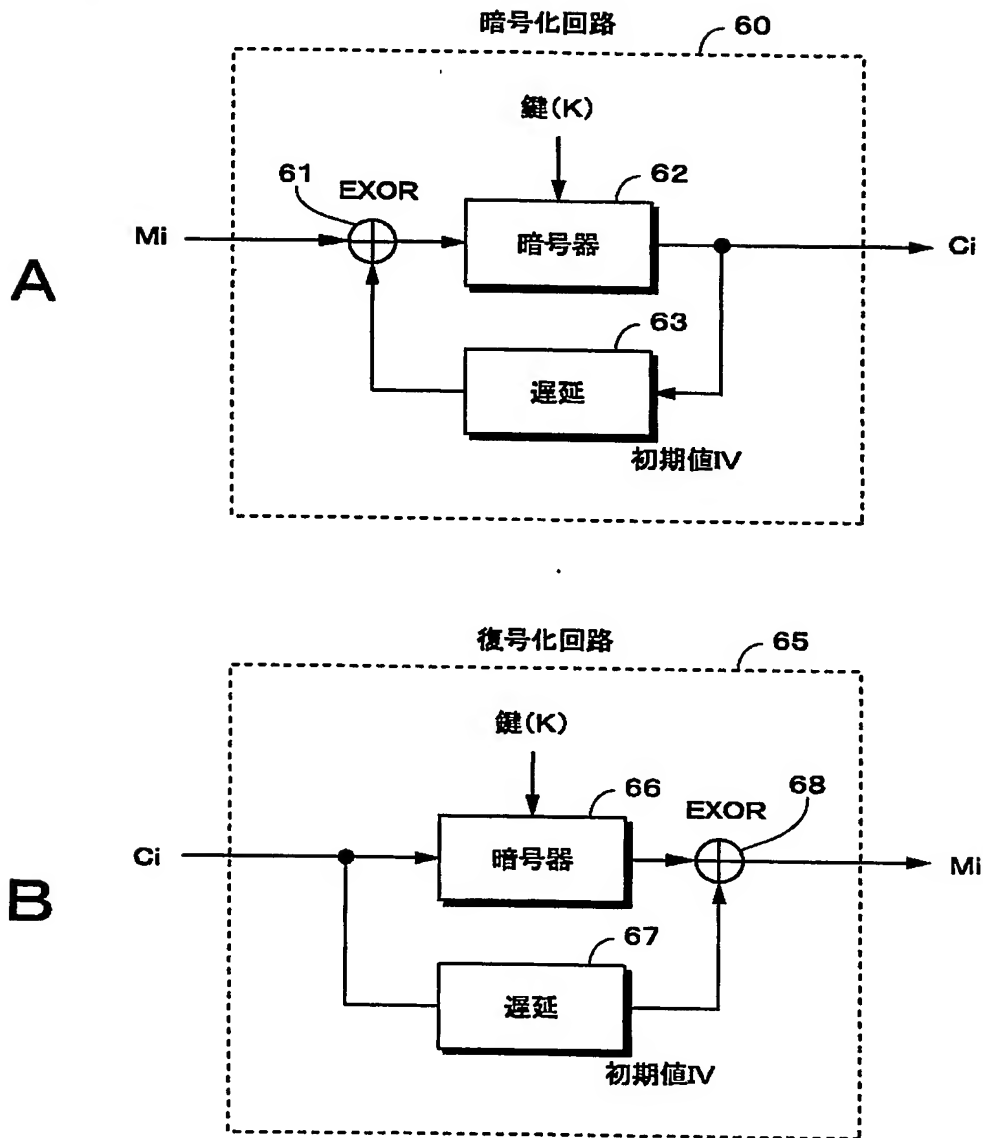




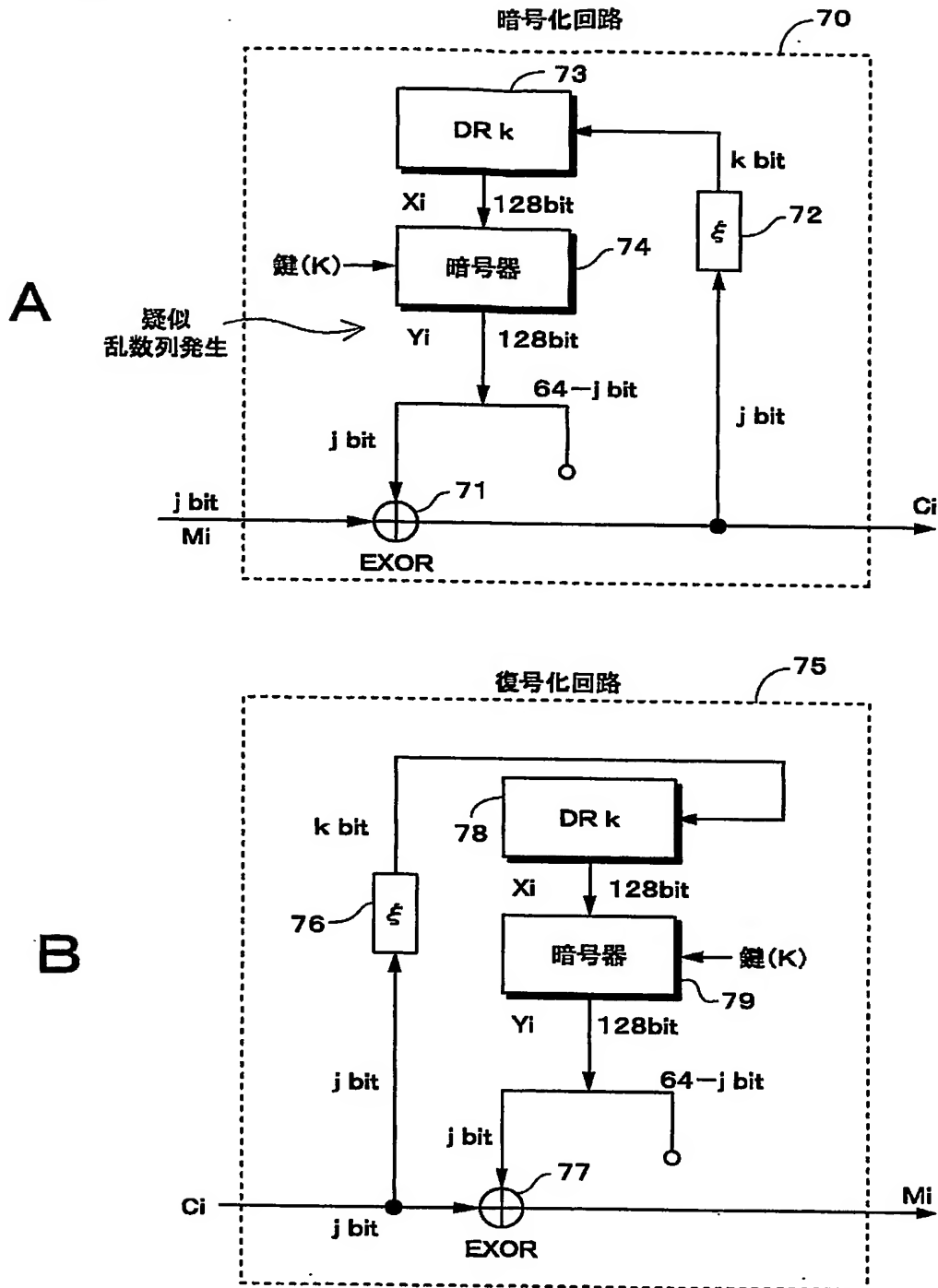
【図 6】



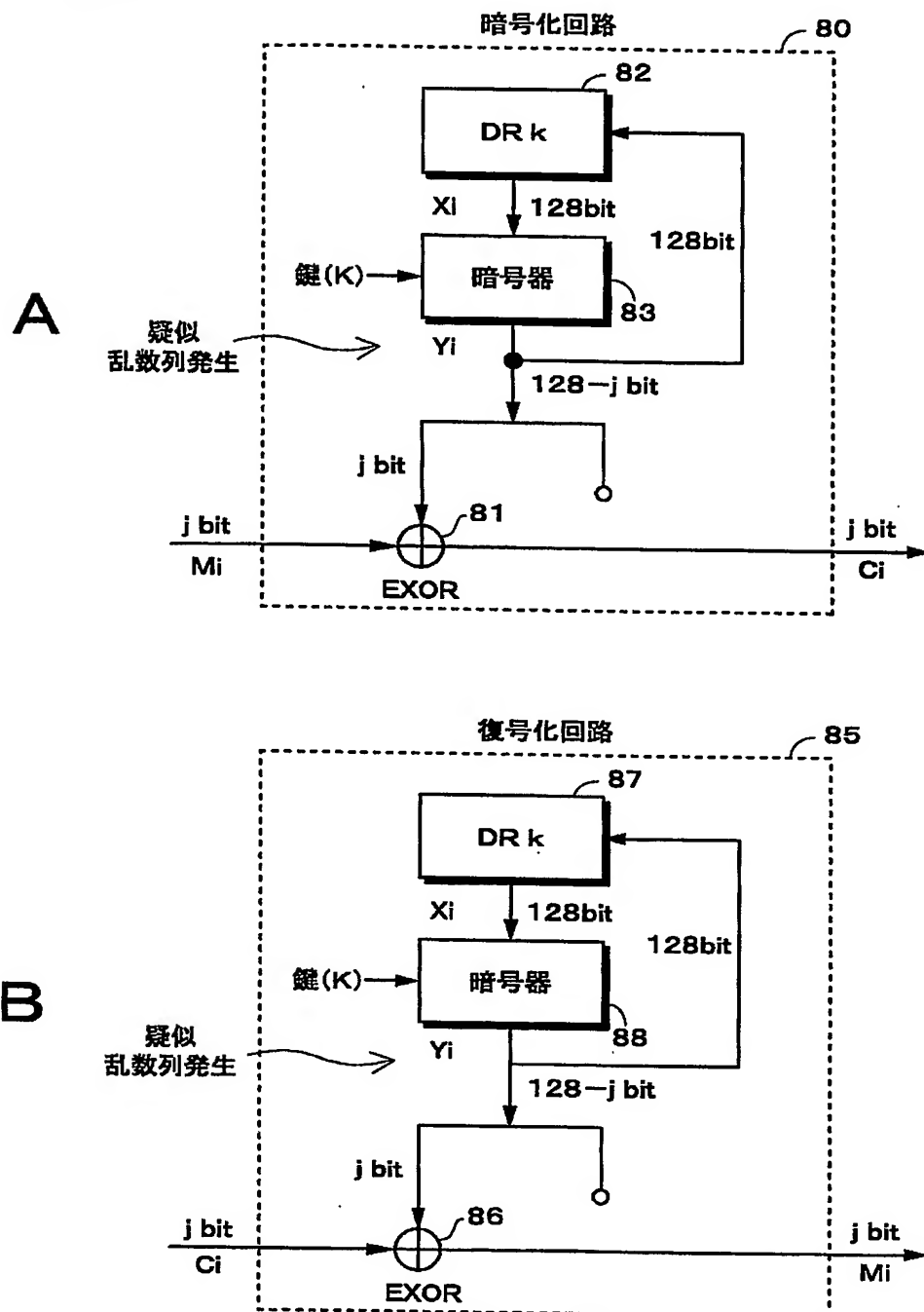
【図 7】



【図 8】

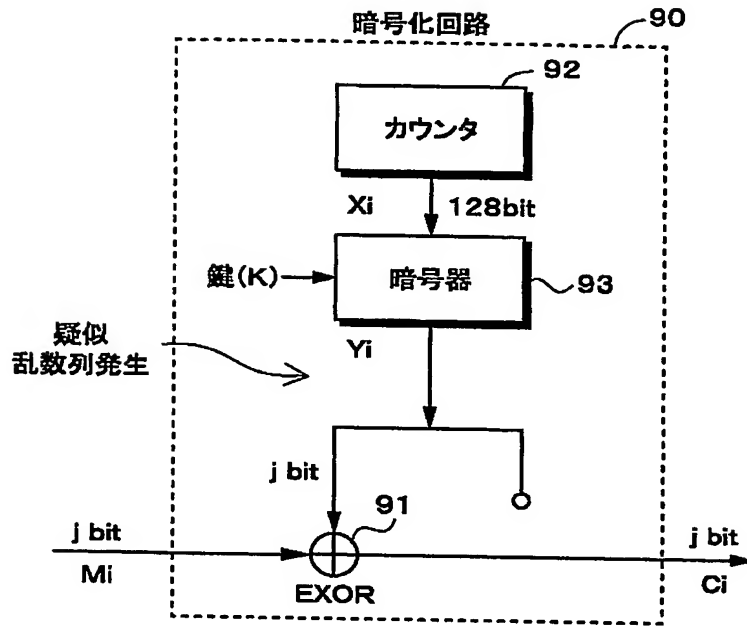


【図 9】

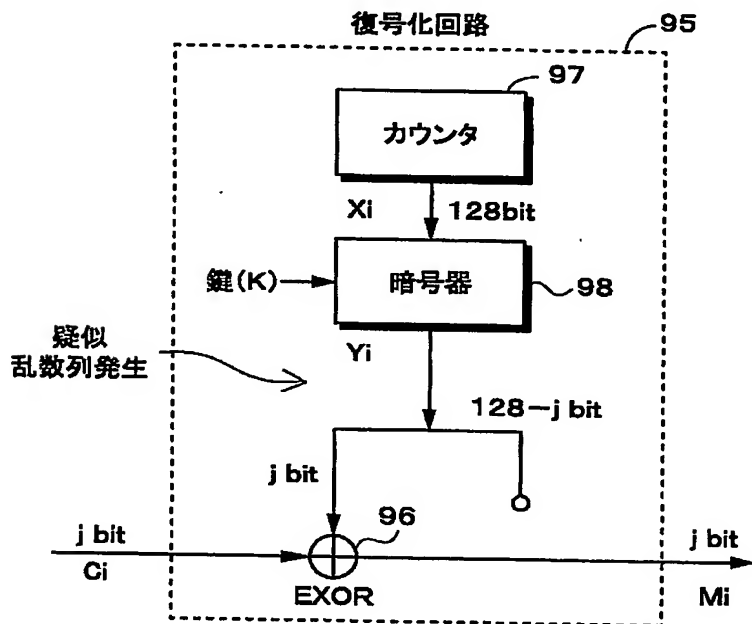


【図 10】

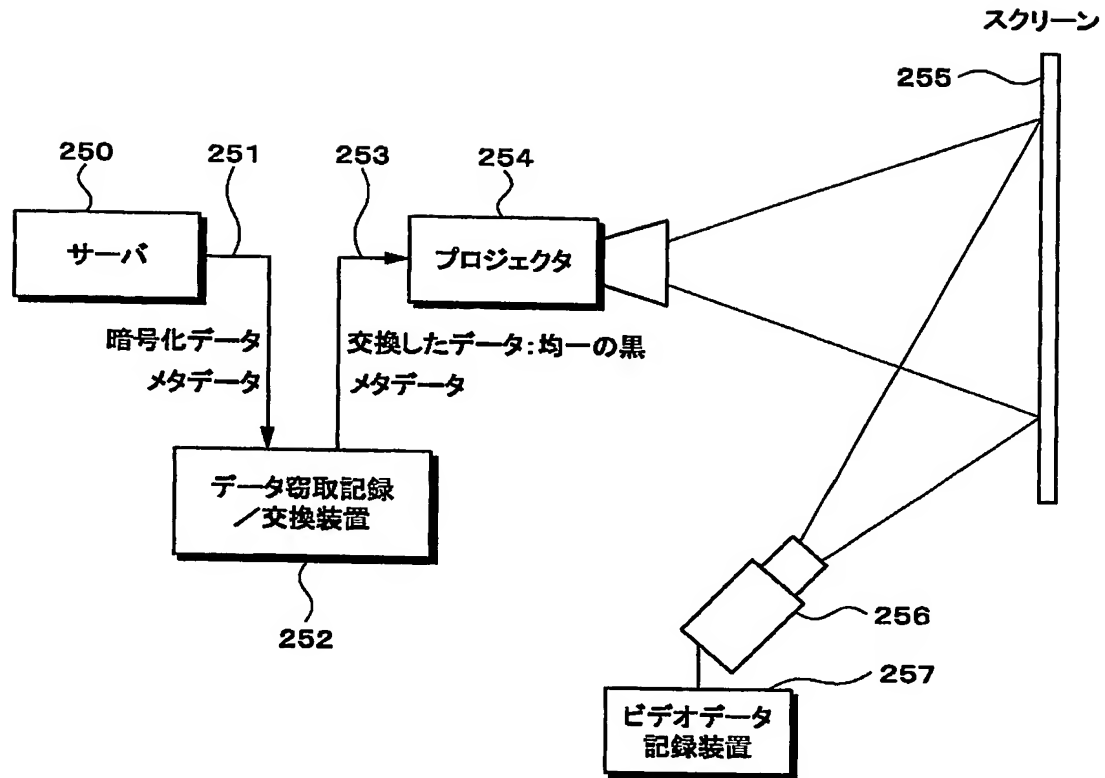
A



B



【図 11】



## 【書類名】 要約書

## 【要約】

【課題】 秘守性に優れ、エラーから完全に復帰できる暗号化を行う。

【解決手段】 入力映像データがE X O R 1 0 0で疑似乱数列と演算されて得られた暗号化データがF F 1 0 1にホールドされ、ライン毎にリセットされる。カウンタ1 0 2及び1 0 3は、夫々ライン毎及びフレーム毎に計数され、フレーム毎及びプログラムの先頭でリセットされる。暗号器1 0 5は、固定値をホールドするF F 1 0 4、カウンタ1 0 3、1 0 2及びF F 1 0 1の出力を鍵（K）を用いて暗号化して疑似乱数列を発生させ、シフトレジスタ1 0 6でビット列を分割する。シフトレジスタ1 0 6の出力と入力映像データとがE X O R 1 0 0で演算され、暗号化データが得られる。暗号出力をフィードバックするので同一データの連続入力を利用したデータ窃取が行えないと共に、フィードバックする暗号出力がライン毎にリセットされるので、エラーから完全に復帰できる。

【選択図】 図3

特願 2 0 0 3 - 2 7 3 9 4 8

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**